NETHEMBA. S R.O., GRÖSSLINGOVÁ 2503/62
811 09 BRATISLAVA

Posúdenie bezpečnosti chráneného dátového úložiska (CHDÚ): Otázky a odpovede

O spoločnosti Nethemba

Nethemba je slovenská IT bezpečnostná spoločnosť založená v roku 2007, špecializujúca sa primárne na bezpečnosť webových a mobilných aplikácií a penetračné testy. Tvoria ju špecialisti s dlhoročnými skúsenosťami v oblasti IT bezpečnosti a svetovými bezpečnostnými certifikátmi (OSCE, OSCP, CISSP). Sme experti na tvorbu komplexných bezpečnostných auditov podľa OSSTMM metodológie ako aj detailných bezpečnostných auditov webových aplikácií podľa testovacej príručky OWASP, tiež sme spoluautori aktuálnej testovacej príručky OWASP v4. Okrem našej špecializácie na bezpečnosť webových a mobilných technológií sa špecializujeme aj na externé, intranetové a lokálne systémové audity, digitálne forenzné analýzy, audity bezdrôtových sietí, návrh ultra-bezpečných, vysoko-dostupných a škálovateľných systémov, cloud computing či školenia v oblasti bezpečnosti pre vývojárov a IT administrátorov.
Medzi naše špeciality patrí bezpečnosť RFID/NFC technológií, hĺbková analýza a tvorba exploitov, bezpečnostné audity SAP systémov či bezpečnosť TETRA a GSM sietí. Venujeme sa tiež bezpečnostnému výskumu v rôznych oblastiach, ktorý aj finančne podporujeme.
Ako prví na svete sme zverejnili „offline“ Mifare Classic cracker, ktorý umožňuje prelomiť viac ako miliardu používaných čipových kariet Mifare Classic.
Súčasne sme odhalili vážne zraniteľnosti v SMS lístkoch používaných vo veľkých stredoeurópskych mestách (Praha, Bratislava, Viedeň, Varšava, Košice), ako aj v mobilnom SMS parkovaní.
Začiatkom roka 2015 sme realizovali tiež rozsiahlu analýzu bezpečnosti platobných NFC kariet.
Aktívne sa venujeme aj ochrane digitálne súkromie (viac informácií na www.chrantesvojesukromie.sk a www.chrantesvesoukromi.cz).

Bezpečnosti sa aktívne venujeme pravidelnými príspevkami na rôznych svetových konferenciách.
Od roku 2014 každoročne organizujeme so spoločnosťou ESET vlastnú IT bezpečnostnú konferenciu Cypherconf.

Ako firma pôsobíme tiež na nemeckom (Nethemba GmbH) a španielskom trhu (Nethemba SA).

Aktuálne informácie zo sveta bezpečnosti reflektujeme na našich sociálnych sieťach:
https://facebook.com/nethemba
https://twitter.com/nethemba
https://www.linkedin.com/company/nethemba

Čo je eKasa?

eKasa predstavuje systém on-line zasielania pokladničných dokladov vystavených na registračných pokladniach (ktoré používajú podnikatelia na evidenciu hotovosti) na server Finančnej správy SR. Každý vystavený doklad na pokladni sa ešte pred samotnou tlačou zašle na server eKasa – zasielajú sa základné údaje bločku (hlavička) a aj jednotlivé položky. Tým získava finančná správa prehľad o každom vystavenom doklade v reálnom čase.

Čo je CHDÚ?

eKasu na strane podnikateľa tvorí pokladničný program eKasa klient (PPEKK) – tým je myslený firmvér pokladnice, prípadne samostatný softvér vo forme napr. DLL knižnice. Ďalej eKasu pokladňu z pohľadu zákona tvorí chránené dátové úložisko (CHDÚ) – ide o pamäť, do ktorej sa dáta môžu len zapisovať, v žiadnom prípade sa nesmie dať čokoľvek už zapísané pozmeniť, prípadne odstrániť. Túto požiadavku musí splňovať aj samotný výrobca CHDÚ – nesmie existovať nástroj, pomocou ktorého by sa dalo niečo pozmeniť alebo vymazať. PPEKK a CHDÚ z hľadiska certifikácie vždy predstavujú jeden celok, ktorý sa certifikuje spoločne.
Do CHDÚ sa zapisujú všetky vystavené doklady (dátové správy zaslané na server FS), ako aj všetky dáta, ktoré sú zaslané na tlačiareň a následne vytlačené. V prípade výpadku internetu (keď nie je server eKasa dostupný) sa pokladničný doklad vo forme dátovej správy (XML) uloží do CHDÚ (tzv. off-line doklad). Po odstránení problémov s pripojením k serveru FS ich následne pokladňa automaticky odošle, prípadne ich odošle na pokyn obsluhy pokladne. CHDÚ primárne slúži na ochranu ešte neodoslaných dokladov na server eKasa – zabraňuje ich dodatočnej úprave, prípadne úplného vymazania ešte pred odoslaním. Pri vystavení dokladu sa do CHDÚ najskôr ukladá dátová správa (zhodná s tou, ktorá sa posiela na server FS), následne sa ukladá aj tlačová úloha – vygenerovaný pokladničný doklad aj s QR kódom. Špecifikáciu CHDÚ vydala Finančná správa SR a je uvedená v nasledovnom dokumente.

Kde je kritická bezpečnostná zraniteľnosť?

Finančné riaditeľstvo SR: *"Podpisový certifikát podnikateľa (súčasť autentifikačných údajov) musí byť pri podpisovaní dátových správ vyžiadaný len z CHDÚ, ak CHDÚ nebude prístupné, PPEKK nesmie podpísať dátovú správu."*

Chyba niektorých eKasa riešení spočíva v tom, že pokladničný program eKasa klient (PPEKK) neoveruje a za súčasných okolností ani nedokáže overiť autenticitu chráneného dátového úložiska (CHDÚ). Keďže sú dáta v CHDÚ voľne dostupné a zároveň komunikácia medzi PPEKK a CHDÚ nie je šifrovaná, útočník sa môže tváriť ako skutočné CHDÚ. Na demonštráciu uvedenej kritickej zraniteľnosti sme vytvorili emulátor CHDÚ, ktorý 100% emuluje reálne

chránené dátové úložisko. V tomto prípade certifikovaná softvérová pokladňa (PPEKK) vydáva pokladničné bločky naďalej, nikdy ich však nezašle na server Finančnej správy SR (z dôvodu blokovania servera eKasa).

V bezpečnostnej terminológii to znamená, že je možné realizovať tzv. MITM (Man-In-The-Middle) útok medzi PPEKK a CHDÚ.

Je uvedený emulátor k dispozícii na stiahnutie?

Nie. V prípade, že Finančná správa nebude uvedenú zraniteľnosť pokladať za dostatočne kritickú, sme pripravení pre demonštráciu závažnosti zverejniť zdrojové kódy emulátora.

Čo všetko dokáže uvedený emulátor CHDÚ?

Okrem vyhotovovania falošných off-line dokladov je možné emulátor použiť aj na opätovnú tlač originálnych dokladov (v tejto verzii je možné tlačiť originál posledného dokladu). Stačí pripojiť CHDÚ akéhokoľvek dodávateľa PPEKK, ktorý používa CHDÚ od firmy CHDÚ, s.r.o. Len s malým úsilím je možné doprogramovať tlač akéhokoľvek dokladu (originálu). Týmto si môžu podnikatelia napr. po skončení mesiaca navzájom zapožičať CHDÚ a vytlačiť si do nákladov toľko dokladov, koľko len potrebujú. Z takýchto dokladov si môžu uplatniť aj odpočet DPH – kontrolný výkaz DPH, ktorý by mohol takéto praktiky odhaľovať, sa podrobne (dokladovo) nezaoberá drobným predajom, ale len faktúrami.

Dokáže bežný zákazník odhaliť, že mu bol vydaný falošný doklad eKasa pokladne, ktorá používa CHDÚ emulátor?

Nie. Oficiálna aplikácia 'Over doklad' len vypíše, že ide o nezaevidovaný doklad, teda čaká sa na jeho zaevidovanie. Na základe hashu, ktorý daný QR kód na doklade obsahuje nie je možné zistiť či ide o platný alebo neplatný doklad, pokým nebol poslaný na server Finančnej správy.

Dokáže Finančná správa na základe obsahu vydaných falošných dokladov z eKasa pokladne identifikovať, ktorý podnikateľ používa eKasu s CHDÚ emulátorom?

Nie. Keďže v tomto prípade samotný obsah je plne pod kontrolou podnikateľa. A môže naň vytlačiť akýkoľvek falošný obsah (napríklad aj údaje svojej konkurencie).

Dokáže Finančná správa zistiť, že podnikateľ dlhodobo používa eKasu s CHDÚ emulátorom?

Bez toho, aby robili opakované kontrolné nákupy, tak nie. V tomto prípade sa totiž do CHDÚ nič neukladá a na servery Finančnej správy nič neposiela.

Ukážka zdrojového kódu emulátora CHDÚ - úprava dokladu tesne pred tlačou

```
index = text.IndexOf("PKP:");
if (index > 0)
{
    // Zneplatniť PKP (elektronický podpis) - pregenerovať náhodnými znakmi
    int index2 = text.IndexOf("==", startIndex: index);
    if (index2 <= 0)
        // Väčšinou končí PKP ==
        // avšak ak nie, dĺžku kódu PKP nastaviť natvrdo (certifikovaná PPEKK tam však môže vkladať formátovacie znaky CRLF)
        index2 = 344;// --- Maximálna dĺža

    Random rand = new Random();
    string availableChars = "0123456789AaBbCcDdEeFfQqGgHhIiJjKkLlMmNnOoPpRrSsTtUuVvZzXxYyWw+/";

    for (var i = index + 4; i <= index2 - 1; i++)
    {
        int value = Strings.Asc(text[i]);
        if (value < 48 | value > 122)
            // Nečitateľný znak, napr. formátovací, ESC sekvencia a podobne
            continue;

        newChar = availableChars.Substring(rand.Next(0, availableChars.Length - 1), 1);
        text = text.Substring(0, i) + newChar + text.Substring(i + 1);
    }
}

// ''''''''''''''''''''''''''''''''''''''''''''
// ZNEPLATNIŤ OKP (OVEROVACÍ KÓD PODNIKATELA) '
// ''''''''''''''''''''''''''''''''''''''''''''
index = text.IndexOf("OKP:");
if (index > 0)
{
    // Zneplatniť OKP (overovací kód pokladne) - pregenerovať náhodnými znakmi, musí sa však zameniť aj v QR kóde
    List<string> ListOKPOriginal = new List<string>();
    List<string> ListOKPFake = new List<string>();

    Random rand = new Random();
    string PartialOKPOriginal = string.Empty;
```

Aký je dopad uvedenej zraniteľnosti?

Ktokoľvek, kto namiesto reálneho chráneného dátového úložiska (CHDÚ) použije emulátor, tak dokáže svojím zákazníkom vystavovať oficiálne vyzerajúce bločky, ktoré nikdy nebudú zaslané do Finančnej správy.

U koľkých dodávateľov certifikovaných riešení by bolo možné tento emulátor použiť?

Momentálne je to asi 20 výrobcov PPEKK, čo predstavuje približne polovicu z celkového počtu certifikovaných riešení.

Na riešenie od firmy CHDÚ s.r.o. sa vzťahuje výnimka – nemusí šifrovať komunikáciu medzi PPEKK a CHDÚ. Znamená to, že zapnutie šifrovania tento bezpečnostný problém vyrieši?

Nešifrovaná komunikácia je závažný bezpečnostný problém. Zavedenie šifrovania zvyšuje bezpečnosť len čiastočne. Zdanlivo bezpečné riešenie by mohla predstavovať napríklad

"challenge-response" autentifikácia, kedy na PPEKK a CHDÚ bude zdieľané tajomstvo a PPEKK dokáže challenge-response protokolom overiť, či CHDÚ dané tajomstvo pozná a teda či ide alebo nejde o emulátor. V tomto prípade aplikácia PPEKK by musela byť špeciálne zabezpečená a obsahovať kľúčový materiál, ktorý potrebuje na overenie "pravého CHDÚ" (buď uložený v samostatnom súbore alebo "hardkodovaný" v samotnom spustiteľom súbore). Principiálne to pôjde ale vždy prelomiť reverzným inžinierstvom a vycrackovať - teda upraviť tak, aby nedokázala rozpoznať či komunikuje s reálnym alebo emulovaným CHDÚ. **Takže MITM útok vždy pôjde realizovať.** Otázkou bude len cena takéhoto útoku (najbezpečnejšie riešenie je mať "custom" počítač a vynucovať TPM/overovanie kontrolných súčtov od samotného bootovania a až po spustenie akéhokoľvek programu, čo je v súčasnej situácii zrejme nepoužiteľné. Ako príklad môžeme použiť napríklad iPhone s keychain).

Ak celé riešenie beží na operačnom systéme, nad ktorým má používateľ plnú kontrolu (čo má) a má možnosť modifikovať a implementovať "backdoory" do systémových knižníc, tak dokáže ovplyvňovať správanie PPEKK a CHDÚ nezávisle od toho, či sú štátom „certifikované a bezpečné" alebo nie.

Nepomôže, keď namiesto komunikácie cez sériovú konzolu sa použije Bluetooth?

Nie. MITM útok na Bluetooth sa dá rovnako dobre realizovať.

Aké je podľa Vás teda riešenie?

Aby uvedený MITM útok nebolo možné realizovať, respektívne, aby náklady naň boli vysoké, tak PPEKK a CHDÚ by malo byť integrované spolu ako tzv "trusted hardware" s pamäťou, z ktorej nebude možné načítať akýkoľvek kľúčový materiál a intervenovať do internej komunikácie PPEKK a CHDÚ. Za súčasných okolností toto riešenie je zrejme extrémne drahé a plošne nenasaditeľné.

Znamená to, že eKasa je podľa Vás menej bezpečná ako pôvodné registračné pokladnice?

Bohužiaľ áno. Vyhotovovanie falošných bločkov je na eKasa jednoduchšie. Pôvodné pokladne boli chránené aspoň plombou servisného technika, pri eKase môže mať podnikateľ ľubovolný počet "čiernych" pokladníc, ktoré pri kontrole neodhalí ani pracovník Finančnej správy (klasické plomby už neexistujú). Identifikačné a autentifikačné údaje môže podnikateľ nahrať súčasne do viacerých pokladníc, z ktorých vlastne ani nie je možné určiť, ktorá je "tá pravá" a ktorá "čierna". Na "čiernej" môže neobmedzene vyhotovovať off-line doklady, ktoré sa nikdy na Finančnú správu neodošlú.

Výhodou systému eKasa je elektronické podpisovanie bločkov samotným podnikateľom (jeho autentifikačnými údajmi). Z podpisu je možné dokázať, či daný bloček skutočne vyhotovil konkrétny podnikateľ na konkrétnom certifikovanom pokladničnom riešení.
Pri použití emulátora to tak ale bohužiaľ nie je. Emulátor dokáže pri tlači bločku nahradiť pravý podpis falošným (je to zmes náhodných znakov), pričom je upravený aj samotný QR kód.

Vyhotovenie offline bločku s falošným podpisom tak úplne znemožňuje finančnej správe dokázať podnikateľovi, že daný doklad vyhotovil skutočne on (samozrejme pokiaľ nie je prichytený priamo pri predaji).

Aké opatrenia by bolo potrebné prijať proti vystavovaniu falošných bločkov?

Myslíme si, že Finančná správa sa nesprávne zameriava na kontrolu nad pokladničnými systémami pre vystavovanie bločkov. Vystaviť falošný bloček totiž môže akýkoľvek program spustený na počítači, napr. aj textový editor. Naviac reverzným inžinierstvom či inými hackerskými technikami bude možné vždy prinútiť eKasu vytvárať falošné bločky (v súčasnosti to platí pre akékoľvek riešenie eKasy). Odporúčame sa preto radšej zamerať na opačnú stranu a to na kontrolu už vystavených dokladov. Snažiť sa získať kontrolu nad vystavovaním falošných bločkov je totiž boj Finančnej správy s veternými mlynmi. Bohužiaľ vždy to zaplatia podnikatelia, ktorí uvedené náklady prenesú na zákazníkov. Finančnej správe sa to nepodarilo pred niekoľkými rokmi pri zavedení fiškálnych pokladníc a pri súčasnom stave bezpečnosti sa jej to nepodarí ani po zavedení eKasy.